REMARKS

This is a response to the Office Action dated January 23, 2003 and the Notice of Non-Responsive Amendment mailed May 14, 2003. Claims 1-67 are pending in the application. In the Office Action, Claims 1-67 were rejected under 35 U.S.C. § 102(b) or (e) as being anticipated by either "Tapping IED Data to Find Transmission Faults", IEEE, 4/1999 ("Peterson"), U.S. Patent Application Publication No. 2002/0091784 ("Baker") or U.S. Pat. No. 6,259,972 ("Sumic").

The rejections from the Office Action of January 23, 2003 and the omissions noted in the Notice of Non-Responsive Amendment of May 14, 2003 are discussed below in connection with the various claims. No new matter has been added. Reconsideration of the application is respectfully requested in light of the following remarks.

I. AMENDMENTS TO THE SPECIFICATION

With this response, the Specification has been amended. This amendment adds no new matter and is supported by the Specification. In particular, the exemplary XML program code has been amended to correct typographic errors in the XML tags. One of ordinary skill in the art would appreciate that XML code requires underscores in place of spaces in XML tag codes.

II. REJECTIONS UNDER 35 U.S.C. § 102(b) or (e)

Independent Claims 1, 34, 51, 53, 54 and 59 were rejected pursuant to 35 U.S.C. § 102(b) or (e) as being anticipated by either Peterson, Baker or Sumic. With this response, claims 34 and 54 have been amended for clarity. These amendments are supported by the specification and no new matter has been added. Applicants submit that neither Peterson, Baker or Sumic anticipate independent claims 1, 34, 51, 53, 54 or 59, as amended, as each of the cited references fails to disclose all of the elements of these claims.

Independent Claim 1, relates to an electrical power management architecture including at least one intelligent electronic device ("IED") coupled with a portion of an electrical power system and further coupled with an internal network and a firewall that couples the internal network with an external network. The architecture further includes a network interface operative to *facilitate communications initiated by the IED* through the firewall to the external network.

Independent Claim 34, as amended, relates to an electric power management architecture. The architecture includes at least one IED coupled with a portion of an electrical power system and further coupled with an internal network. The architecture further includes a firewall operative to couple the internal network with an external network, and a communications interface operative to facilitate communications of the IED with a transport box. The transport box includes a network interface and is operative to facilitate communication of power management data through the firewall. The network interface is operative to *initiate communications of the power management data from the internal network to the external network via the firewall on behalf of the IED.*

Independent Claim 51 relates to an electrical power management architecture including at least one IED coupled with a portion of an electrical power system and further coupled with an internal network. In addition, the architecture includes a firewall operative to couple an external network with the internal network and a mail server coupled with the internal network and operative to receive, process and forward messages from the IED to the external network. The architecture further includes "a network interface operative to couple the IED with the internal network and further operative to communicate with the mail server, the mail server being operative to communicate through the firewall, and further wherein the mail server is *operative to initiate communications* of at least one of the electronic mail messages from the internal network to the external network."

Independent Claim 53, as amended, relates to an electrical power management architecture for managing an electrical power distribution system. The architecture includes a network and at least one IED coupled with a portion of said electrical power distribution system and further coupled with said network. Each of the at least one IED is operative to implement a power management function in conjunction with the portion of said electrical power distribution system, the power management function operative to respond to at least one power management command and generate power management data. Each of the at least one IED includes a first network interface operative to couple the at least one IED with the network and facilitate transmission of the power management data and receipt of the at least one power management command over the network. Each of the at least one IED further includes a security module coupled with the first network interface and operative to prevent unauthorized access to the power management data and *a protocol stack, the protocol stack including an application layer comprising at least one application operative to punch through a firewall to facilitate said*

transmission of said power management data. The architecture further includes a power management application coupled with the network and operative to receive and process the power management data from the at least one IED and generate the at least one power management command to the at least one IED to implement the power management function.

Independent Claim 54, as amended, relates to a method of communicating power management data in an electrical power management architecture between an internal network and an external network, the internal network being coupled with the external network by a firewall. The method includes: "monitoring a portion of an electrical power distribution system with at least one intelligent electronic device ("IED"), the at least one IED further being coupled with the internal network;" "generating power management data by the at least one IED corresponding to said monitoring;" "*initiating a first communications of the power management data by the at least one IED to a receiver*, the receiver being coupled with the external network;" and "facilitating the initiated first communications through the firewall to the external network for delivery to the receiver." (emphasis added).

Independent Claim 59 relates to a method of communicating power management data in an electrical power management architecture between an internal network and an external network, the internal network being coupled with the external network by a firewall through which communications between the internal network and external network must travel. The method includes: "monitoring a portion of an electrical power distribution system with at least one intelligent electronic device ("IED"), the at least one IED further being coupled with the internal network;" "generating power management data by the at least one IED corresponding to the monitoring;" "*initiating a first communications of the power management data by the at least one IED to a receiver*, the receiver being coupled with the external network;" "configuring the internal network to allow the first communications to be transmitted to the external network via the firewall;" and "transmitting the initiated first communications through the firewall to the external network for delivery to the receiver." (emphasis added).

Peterson discloses methods to automatically determine the location of faults in an electrical power system using oscillographic or phasor data from IEDs and communicate the information from local SCADA systems to centralized SCADA systems for display on a variety of interfaces and further processing as necessary. *See* Peterson, page 36-37 and page 38, left column bottom.

Baker discloses a "method and interface module for communicating messages with a remote location and to provide access to an at least one intelligent electronic device (IED) operably connected to a communication network. The interface module is comprised of a central processing unit and an operating system operating the central processing unit. A network interface is operably connected with the communication network. A protocol task processes communication on the network according to a protocol stack. A set of application tasks communicates with the protocol task for responding to an incoming message from the communication network and initiating an outgoing message to the communication network. An interconnection bus with an interface driver is operably connected with the at least one IED." *See* Baker, Abstract.

Sumic discloses a "method and system for processing and disseminating utility outage information is disclosed. In response to the receipt of new data in the form of events, the data is mapped into a geographic information system and transmitted to selected recipients, or subscribers. Each subscriber has one or more areas of interest that define the information it receives. Each subscriber also has a security classification that further defines the information it may receive as well as the subscriber's ability to trigger events, or update the outage information. The mechanism of the invention employs multiple ways of disseminating the information. A subscriber may request that updated information be sent to the subscriber in response to a subscriber's request. Alternatively, the subscriber may request that updated information be automatically transmitted to the subscriber when updated information is received." *See* Sumic, Abstract.

A. Independent claims 1, 53, 54 and 59

Peterson, Baker and Sumic all fail to disclose that the IED initiates communications from an internal network to an external network via a firewall, as claimed in claims 1, 54 and 59. Similarly, Peterson, Baker and Sumic all fail to disclose that the IED includes an application as part of the application layer of a protocol stack which is capable of "punching through" a firewall to facilitate the transmission of power management data generated by the IED, as claimed in claim 53. Peterson discloses that the IED communicates via an intermediary "Web Server/Fault Vision Application" through the firewall. *See* Peterson, Page 41, Figure 7. Further Peterson describes that the "Web Server/Fault Vision Application" initiates the communication to the IED as needed or automatically. *See* Peterson, Page 40, the section entitled "Automatic Data

Retrieval". Baker merely discloses firewalls in general terms, i.e. that the network may contain "specialized infrastructure components such as routers and firewalls". *See* Baker, para. 5. Sumic also discloses a firewall 618 only in general terms as an intermediary security device between the Internet server 614 and the Internet 616. *See* Sumic, Figure 6 and Col. 8, lines 39-56.

Peterson, Baker and Sumic all fail to disclose that the IED initiates communications through the firewall, from the internal to the external network, or that the IED is capable of punching through a firewall. As this element is not disclosed by the cited references, Applicants submit that claims 1, 53, 54 and 59 are not anticipated by Peterson, Baker or Sumic.

B. Independent claim 34

Peterson, Baker and Sumic all fail to disclose that the transport box initiates communications of power management data via a firewall, as claimed in claim 34.

As previously explained Peterson discloses that the IED communicates to the "Web Server/Fault Vision Application" before the communication is transmitted through the firewall. Further, this communication is initiated by a request by the operator to "request a fault location calculation for a transmission line by selecting a single button o the main operator display." *See* Peterson, Page 40, the section entitled "Automatic Data Retrieval". As previously explained, Baker merely discloses firewalls in general terms, i.e. that the network may contain "specialized infrastructure components such as routers and firewalls". *See* Baker, para. 5. Sumic discloses the "pulling" and "pushing" of data from the OMS to recipients but does not disclose the pushing of power management data through a firewall. *See* Sumic, Col 6, lines 39-61.

Therefore, Peterson, Baker and Sumic all fail to disclose that the transport box initiates communications through the firewall, from the internal to the external network via the firewall. As this element is not disclosed by the cited references, Applicants submit that claim 34 is not anticipated by Peterson, Baker or Sumic.

C. Independent claim 51

Peterson, Baker and Sumic all fail to disclose a mail server coupled with an internal network to an external network via a firewall, as claimed in claim 51. As previously explained, Peterson discloses that the IED communicates to the "Web Server/Fault Vision Application" before communication is transmitted through the firewall. This "Application" is not described as being a mail server. *See* Peter, Page 40, the section entitled "Automated Fault Location

Processing". As previously explained, Baker merely discloses firewalls in general terms, further no disclosure of a mail server in combination with the proposed invention is made in the application. Likewise, Sumic also discloses a firewall in general terms but also does not describe or mention a mail server in combination with the disclosed invention.

Therefore, Peterson, Baker and Sumic all fail to disclose a mail server initiates communications through the firewall, from the internal to the external network via the firewall. As this element is not disclosed by the cited references, Applicants submit that claim 51 is not anticipated by Peterson, Baker or Sumic.

For at least these reasons, Claims 1, 34, 51, 53, 54 and 59 are not anticipated by either Peterson, Baker or Sumic. Accordingly, Applicants request that the Examiner withdraw this rejection of independent Claims 1, 34, 51, 53, 54 and 59.

D. Dependent claims

Dependent Claims 2-33, 35-50, 52, 55-58 and 60-67 were also rejected pursuant to 35 U.S.C. § 102(b) or (e) as being anticipated by Peterson, Baker or Sumic. Dependent claims 2-33, 35-50, 52, 55-58 and 60-67 should be allowed for the reasons set out above for the independent claims. Applicants therefore request that the Examiner withdraw this rejection of these claims.

In addition, additional limitations of these dependent claims also distinguish over the cited references. For example, none of the cited references discloses: wherein the firewall is operative to selectively restrict selected protocols communicated between the external network and the internal network, as claimed in claim 2; wherein the network interface is further operative to facilitate receipt of the first power management data from the external network, as claimed in claim 3; wherein the first power management data is received as at least one electronic mail message, as claimed in claim 4; wherein the first power management data is received as at least one instant message, as claimed in claim 5; wherein the first power management data is communicated as at least one electronic mail message, as claimed in claim 8; wherein the first power management data is communicated as at least one instant message, as claimed in claim 9; wherein the external network further comprises an external mail server, the IED being further adapted to retrieve second power management data from the external mail server, as claimed in claim 10; wherein the IED retrieves the second power management data

using a POP3 protocol, as claimed in claim 11; wherein the second power management data is retrieved as at least one electronic mail message, as claimed in claim 12; wherein the IED is capable of being configured to facilitate receipt of the power management data from the external mail server, as claimed in claim 13; wherein the internal network is further coupled with an internal mail server, the IED adapted to retrieve the first power management data from the internal mail server, as claimed in claim 14; wherein the network interface is further coupled with a security module, the security module operative to prevent unauthorized access to the power management data, as claimed in claim 16; wherein the security module further comprises a second firewall, as claimed in claim 17; a security module coupled with the network interface, the security module further comprising an encryption application operative to encrypt the first power management data prior to communication, as claimed in claim 18; a security module coupled with the network interface, the security module operative to authenticate second power management data received from the external network, as claimed in claim 19; wherein the security module is operative to decrypt the second power management data received from the external network, as claimed in claim 20; the network interface using at least one application, wherein the application comprises a SMTP client, as claimed in claim 21; the network interface comprising at least one application, wherein the application comprises an instant messaging protocol, as claimed in claim 22; the network interface comprising at least one application, wherein the application comprises a hypertext transport protocol ("HTTP") tunneling application, as claimed in claim 23; the network interface comprising at least one application, wherein the application communicates the power management data on a scheduled basis, as claimed in claim 24; wherein the IED retrieves a timestamp from a time server, the timestamp operative to timesync the IED, as claimed in claim 25; the network interface comprising at least one application operative to communicate the power management data on a scheduled basis, the scheduled basis being authenticated from the timestamp, as claimed in claim 26; the network interface comprising at least one application operative to communicate the power management data on an event driven basis, as claimed in claim 27; wherein the first power management data comprises a power management command, as claimed in claim 28; wherein the first power management data is in extensible markup language ("XML") format, as claimed in claim 29; wherein the first power management data is in comma-separated value ("CSV") format, as claimed in claim 30; wherein the electrical power system comprises a generator, as claimed in claim 32; wherein the firewall is adapted to restrict communications from the internal network to

B

the external network, as claimed in claim 35; wherein the firewall is operative to restrict selected protocols between the external network and the internal network, as claimed in claim 36; wherein a security module is coupled with the network interface, the security module operative to prevent unauthorized access to the power management data, as claimed in claim 37, wherein the IED transmits an electronic pulse to the transport box, the transport box converting the electronic pulse into power management data, as claimed in claim 39; wherein the transport box converts the power management data to XML format, as claimed in claim 40; wherein the communications comprises at least one electronic mail message, as claimed in claim 41; wherein the communications comprises at least one instant message, as claimed in claim 42; wherein the network interface is further coupled to a security module, the security module further comprises an encryption application operative to encrypt the power management data prior to transmission of the power management data, as claimed in claim 43; wherein the transport box is further operative to receive an external electronic mail message from the external network, the IED further operative to communicate with the transport box and retrieve the external electronic mail message from the transport box, as claimed in claim 44; wherein a second network interface is operative to couple the IED with the internal network, as claimed in claim 45; wherein the communications comprises HTTP tunneling, as claimed in claim 46; wherein the IED is a Remote Terminal Unit ("RTU"), as claimed in claim 49; wherein the firewall comprises a proxy server, as claimed in claim 50; wherein the mail server uses a POP3 protocol, as claimed in claim 52; receiving a second communications by the at least one IED from the external network through the firewall, as claimed in claim 55; wherein the first communications comprises at least one electronic mail message, as claimed in claim 56; allowing communications using standard protocols between the internal and external networks by the firewall, as claimed in claim 57; restricting communications using standard protocols between the internal and external networks by the firewall, as claimed in claim 58; configuring an electronic mail server coupled with the internal network to allow the at least one IED to send electronic mail to the external network using the electronic mail server, the electronic mail server being operative to transmit electronic mail messages from the internal network to the external network via the firewall, as claimed in claim 60; configuring the firewall to allow the at least one IED to communicate with a communications server coupled with the external network, as claimed in claim 61; wherein the communications server comprises an electronic mail server, as claimed in claim 62; wherein the communications server comprises an XML server, as claimed in claim 63; wherein the first

communications is formatted in a computer readable format, as claimed in claim 64; wherein the receiver comprises a data processing system operative to receive the first communications and automatically process the power management data, as claimed in claim 65; wherein the initiating is performed in response to an occurrence of an event monitored on the power distribution system, as claimed in claim 66; and wherein the initiating is performed according to a pre-defined schedule maintained by the at least one IED, as claimed in claim 67.

III. NEW CLAIMS

With this response, new dependent Claims 68-96 have been added. These claims add no new matter and are supported by the specification. Applicants submit that as new claims 68-86 depend directly or indirectly from independent claim 1 and new claims 87-96 depend from independent claim 51, these new claims should be allowed for the same reasons discussed above for independent claims 1 and 51 and are, therefore, no not anticipated by Peterson, Baker or Sumic.

In particular, Peterson, Baker and Sumic fail to disclose all of the elements of independent claim 1, as discussed above, plus: wherein the first power management data further comprises an HTTP format, as claimed in claim 68; wherein the first power management data further comprises an XML format, as claimed in claim 69; wherein the first power management data further comprises a SOAP format, as claimed in claim 70; wherein the first power management data further comprises an SSL format, as claimed in claim 71; wherein the first power management data further comprises an NNTP format, as claimed in claim 72; wherein the first power management data further comprises an FTP format, as claimed in claim 73; wherein the first power management data further comprises a MIME format, as claimed in claim 74; wherein the first power management data further comprises an S-HTTP format, as claimed in claim 75; wherein the first power management data further comprises an HTTP format, as claimed in claim 76; wherein the first power management data further comprises an XML format, as claimed in claim 77; wherein the first power management data further comprises a SOAP format, as claimed in claim 78; wherein the IED retrieves the second power management data using an IMAP protocol, as claimed in claim 79; wherein the external network further comprises an external mail server, the IED being further adapted to send the first power management data to the external mail server, as claimed in claim 80; wherein the IED retrieves

the second power management data using an POP3 protocol, as claimed in claim 81; wherein the IED retrieves the second power management data using an IMAP protocol, as claimed in claim 82; further comprising a security module coupled with the network interface, the security module further operative to provide authentication of the first power management data prior to communication, as claimed in claim 83; wherein the internal network is further coupled with a security module, the security module operative to prevent unauthorized access to the power management data, as claimed in claim 84; wherein the IED further comprises the security module, as claimed in claim 85; and wherein the timesync further comprises the NTP protocol, as claimed in claim 86.

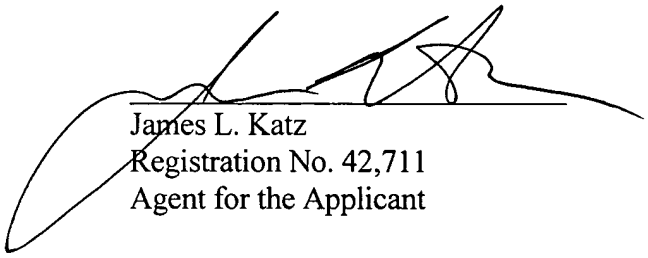
Further, Peterson, Baker and Sumic fail to disclose all of the elements of independent claim 51, as discussed above, plus: wherein the mail server uses an IMAP protocol, as claimed in claim 87; wherein the at least one electronic mail messages is encrypted, as claimed in claim 88; wherein the at least one electronic mail messages is decrypted, as claimed in claim 89; wherein the at least one electronic mail messages is authenticated, as claimed in claim 90; wherein the at least one electronic mail messages further comprises an SMTP format, as claimed in claim 91; wherein the at least one electronic mail messages further comprises an XML format, as claimed in claim 92; wherein the at least one electronic mail messages further comprises a CSV format, as claimed in claim 93; wherein the at least one electronic mail messages further comprises a MIME format, as claimed in claim 94; wherein the at least one electronic mail messages further comprises an IMAP format, as claimed in claim 95; and wherein the at least one electronic mail messages parameters conform to the requirements of the external mail server, as claimed in claim 96.

Applicants therefore submit that new claims 68 to 96 are allowable over the cited art.

CONCLUSION

Each of the rejections in the Office Action dated January 23, 2003 and the omissions from the Notice of Non-Responsive Amendment of May 14, 2003 has been addressed and no new matter has been added. Applicant submits that all of the pending claims are in condition for allowance and notice to this effect is respectfully requested. The Examiner is invited to call the undersigned if it would expedite the prosecution of this application.

Respectfully submitted,



James L. Katz
Registration No. 42,711
Agent for the Applicant

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, ILLINOIS 60610
(312) 321-4200